

Prefazione

Scrivere il Bitcoin Book

Mi sono imbattuto per la prima volta in bitcoin a metà del 2011. La mia reazione immediata è stata più o meno "Pfft! Una moneta per nerd!" e l'ho ignorata completamente per altri sei mesi, fallendo nel cogliere la sua importanza. Questa è una reazione che ho visto ripetuta anche tra molte delle persone intelligenti che conosco, e ciò mi consola un pò. La seconda volta che ho ri-incontrato bitcoin, in una discussione di una mailing list, ho deciso di leggere il white-paper scritto da Satoshi Nakamoto, per studiare la sorgente autoritativa e vedere di che si trattasse. Mi ricordo ancora il momento nel quale finii di leggere quelle nove pagine, quando realizzai che bitcoin non era semplicemente una valuta digitale, ma un network basato sulla fiducia che poteva anche fornire le basi per costruire molto di più di semplici valute. La realizzazione che "questa non è una moneta, è un network decentralizzato basato su fiducia," mi ha portato a un viaggio di quattro mesi per divorare ogni frammento di informazione su bitcoin che potevo trovare. Sono rimasto incollato e diventato ossessionato, spendendo 12 o più ore al giorno attaccato allo schermo, leggendo, scrivendo testo e codice e imparando più che potevo. Sono emerso da questo stato di fuga, dimagrito di 9 chili dalla mancanza di pasti costanti, determinato a dedicare tutto me stesso per lavorare su bitcoin.

Due anni più tardi, dopo aver creato un certo numero di piccole startup per esplorare vari servizi e prodotti relativi al Bitcoin, ho deciso che era il momento di scrivere il mio primo libro. Bitcoin mi ha rapito, gettandomi in un frenetico vortice di creatività; è stata la più eccitante tecnologia che ho incontrato da quando c'è internet.

Pubblico di Riferimento

Questo libro è prevalentemente inteso per i programmatori. Se tu sai usare un linguaggio di programmazione, questo libro ti insegnerà come funzionano le monete basate su algoritmi crittografici, come usarle e come sviluppare software che lavori con esse. I primi capitoli sono adatti anche come introduzione approfondita per Bitcoin per i non programmatori e per coloro che cercano di capire il funzionamento interno di Bitcoin e delle crittovalute.

Convenzioni usate in questo libro

Le seguenti convenzioni tipografiche sono usate in questo libro:

Italic

Indica nuovi termini, URLs, indirizzi email, filename, e estensioni.

Larghezza costante

Usata per listati di programmi, come per paragrafi che si riferiscono a elementi di programmi come nomi di funzioni o variabili, database, tipi di dati, variabili d'ambiente, istruzioni e parole chiave.

Larghezza costante in grassetto

Mostra comandi o altro testo che dovrebbe essere digitato letteralmente dall'utente.

Larghezza costante in corsivo

Mostra testo che dovrebbe essere sostituito con valori definiti dall'utente o con valori determinati dal contesto.

TIP | L'icona sta a significare un tip, un suggerimento o una nota generale.

WARNING | Questa icona indica un avvertimento o cautela.

Esempi di Codice

Gli esempi sono illustrati in Python, C++, usando la riga di comando di un sistema operativo Unix-like come Linux o Mac OS X. Tutti i frammenti di codice sono disponibili nel [repository GitHub](#) nella directory *code* del repo principale. Fai un fork del codice del libro, prova gli esempi di codice o sottoporti delle correzioni via GitHub.

Tutti i frammenti di codice possono essere replicati in gran parte dei sistemi operativi con un'installazione minimale di compilatori e interpreti per i rispettivi linguaggi. Dove necessario, forniamo istruzioni d'installazione basilari ed esempi passo-passo dell'output di quelle istruzioni.

Alcuni dei frammenti di codice e degli output sono stati riformattati per la stampa. In tutti questi casi le linee sono state divise da una barra rovesciata (`\`), seguita da un carattere newline. Quando si trascrivono gli esempi si rimuovano questi due caratteri e si uniscano di nuovo le linee; si dovrebbero vedere risultati identici a quelli nell'esempio.

Tutti i frammenti di codice usano dove possibile valori reali e calcoli, in modo che si possa costruire di esempio in esempio e vedere gli stessi risultati in ogni codice si scriva per calcolare gli stessi valori. Per esempio, le chiavi private e le corrispondenti chiavi pubbliche e indirizzi sono tutti reali. Le transazioni di prova, i blocchi, e i riferimenti in blockchain sono stati tutti introdotti nella reale catena dei blocchi bitcoin e sono parte del registro pubblico; dunque si possono consultare in qualsiasi sistema bitcoin.

Riconoscimenti

Questo libro rappresenta gli sforzi e i contributi di molte persone. Sono grato per tutto l'aiuto che ho ricevuto da amici, colleghi ed anche sconosciuti, che si sono uniti in questo sforzo per scrivere il libro tecnico definitivo su crittovalute e bitcoin.

E 'impossibile fare una distinzione tra la tecnologia Bitcoin e la comunità bitcoin, e questo libro è tanto un prodotto di quella comunità quanto è un libro sulla tecnologia Bitcoin. Il mio lavoro su questo libro è stato incoraggiato, acclamato, sostenuto, e premiato da tutta la comunità bitcoin dall'inizio fino alla fine. Più di ogni altra cosa, questo libro mi ha permesso di essere parte di una comunità meravigliosa per due anni e non posso ringraziarvi abbastanza per avermi accettato in questa comunità. Ci sono troppe persone da menzionare per nome, persone che ho incontrato in occasione di conferenze, eventi, seminari, meetup, pizza e piccoli incontri privati, così come molti che comunicavano con me via Twitter, su reddit, su [bitcointalk.org](#), e su GitHub che hanno avuto

un impatto su questo libro. Ogni idea, analogia, domanda, risposta, e spiegazione che si trova in questo libro è stata, ad un certo punto, ispirata, provata, o migliorata attraverso le mie interazioni con la comunità. Grazie a tutti per il vostro sostegno; senza di voi questo libro non sarebbe nato. Sarò per sempre grato di tutto questo.

Il percorso per diventare un autore inizia molto prima del primo libro, naturalmente. La mia prima lingua (e la scuola) era greca, così ho dovuto fare un corso di scrittura inglese correttiva nel mio primo anno di università. Devo ringraziare Diana Kordas, il mio insegnante di scrittura inglese, che mi ha aiutato a costruire la fiducia e le competenze che ho. Più tardi, come un professionista, ho sviluppato le mie capacità tecniche di scrittura sul tema del data center, scrivendo per la rivista *Network World*. Devo ringraziare John Dix e John Gallant, che mi hanno dato il mio primo lavoro di scrittura come editorialista al *Network World* e al mio editore Michael Cooney e il mio collega Johna Fino Johnson che ha curato le mie colonne e le ha rese adatte alla pubblicazione. Scrivere 500 parole a settimana per quattro anni mi ha dato abbastanza esperienza per prendere in considerazione l'idea di diventare un autore. Grazie a Jean de Vera per il suo primo incoraggiamento a diventare un autore e per aver creduto sempre e insistendo sul fatto che avevo un libro in me.

Grazie anche a coloro che mi hanno supportato quando ho sottoposto la mia proposta del libro a O'Reilly, per aver provvisto referenze e aver rivisto la proposta. Un ringraziamento, specialmente a John Gallant, Gregory Ness, Richard Stiennon, Joel Snyder, Adam B. Levine, Sandra Gittlen, John Dix, Johna Till Johnson, Roger Ver, and Jon Matonis. Ringraziamenti speciali a Richard Kagan e Tymon Mattoszek, che hanno revisionato versioni iniziali della proposta e Matthew Owain Taylor, che ha redatto la proposta.

Grazie a Cricket Liu, autore del titolo *DNS O'Reilly e BIND*, che mi ha introdotto a O'Reilly. Grazie anche a Michael Loukides e Allyson MacDonald di O'Reilly, che ha lavorato per mesi per contribuire a rendere questo libro reale. Allyson è stata particolarmente paziente quando le scadenze non sono state mantenute e consegnati in ritardo e di come gli eventi vita siano intervenuti nel nostro programma di lavoro.

Le prime bozze dei primi capitoli sono stati le più difficili, perché Bitcoin è un argomento difficile da dipanare. Ogni volta che ho tirato in ballo la tecnologia bitcoin, ho dovuto tirare tutto la faccenda. Sono più volte rimasto bloccato e un po' scoraggiato mentre lottavo per rendere l'argomento facile da capire e creare una narrazione intorno ad un argomento tecnico così denso. Alla fine, ho deciso di raccontare la storia di bitcoin attraverso le storie delle persone che utilizzano Bitcoin e tutto il libro è diventato molto più facile da scrivere. Devo ringraziare il mio amico e mentore, Richard Kagan, che mi ha aiutato a svelare la storia e superare i momenti di blocco dello scrittore, e Pamela Morgan, che ha esaminato le prime bozze di ogni capitolo e ha fatto le domande più difficili per renderlo migliore. Inoltre, grazie agli sviluppatori del gruppo di San Francisco Bitcoin Meetup Dev e Taariq Lewis, co-fondatore del gruppo, per aver contribuito a testare il materiale in anticipo.

Durante lo sviluppo del libro, ho fatto le prime bozze disponibili su GitHub e invitato il pubblico a commentare. Più di un centinaio di commenti, suggerimenti, correzioni e contributi sono stati presentati in risposta. Tali contributi sono esplicitamente riconosciuti, con i miei ringraziamenti, in [Bozza della Early Release \(Contributi da GitHub\)](#). Un ringraziamento speciale a Minh T. Nguyen, che si sono offerti per la gestione dei contributi GitHub e hanno aggiunto molti contributi significativi. Grazie anche a Andrew Naugler per il design infografica.

Quando il libro era nella fase di bozza, è passato attraverso molti round di revisione tecnica. Grazie a Cricket Liu e a Lorne Lantz per la loro revisione approfondita, commenti e supporto.

Molti sviluppatori bitcoin hanno contribuito ad esempi di codice, recensioni, commenti e incoraggiamenti. Grazie a Amir Taaki e Eric Voskuil per snippet di codice esempio e per i molti commenti di pregio; Vitalik Buterin e Richard Kiss per aver aiutato con la matematica della curva ellittica e altri contributi al codice; a Gavin Andresen per correzioni, commenti e per l'incoraggiamento; a Michalis Kargakis per i commenti, contributi e per lo scritto su btcd; e a Robin Inge per le correzioni degli errori che hanno migliorato la seconda edizione;

Devo tutto l'amore che ho per le parole e per i libri a mia madre, Theresa, che mi ha cresciuto in una casa con libri che potevi trovare a ogni parete. Mia madre mi ha inoltre comprato il mio primo computer nel 1982, anche se si considera una che ha un po paura della tecnologia. Mio padre, Meneleas, un ingegnere civile che ha appena pubblicato il suo libro a 80 anni, era colui che mi ha insegnato il pensiero logico e analitico e mi ha trasmesso un'amore per la scienza e l'ingegneria.

Grazie a tutti per avermi aiutato durante questo viaggio.

Bozza della Early Release (Contributi da GitHub)

Moltri contributor hanno offerto commenti, correzioni e aggiunte alla bozza di pre-release su GitHub. Grazie a tutti i vostri contributi che avete dato a questo libro. Di seguito una lista di noti contributor sul progetto bitcoinbook su GitHub, inclusi i loro GitHub ID tra parentesi:

- Minh T. Nguyen, GitHub editor delle contributions (enderminh)
- Ed Eykholt (edeykholt)
- Michalis Kargakis (kargakis)
- Erik Wahlström (erikwam)
- Richard Kiss (richardkiss)
- Eric Winchell (winchell)
- Sergej Kotliar (ziggamon)
- Nagaraj Hubli (nagarajhubli)
- ethers
- Alex Waters (alexwaters)
- Mihail Russu (MihailRussu)
- Ish Ot Jr. (ishotjr)
- James Addison (jayaddison)
- Nekomata (nekomata-3)
- Simon de la Rouviere (simondlr)
- Chapman Shoop (belovachap)
- Holger Schinzel (schinzelh)
- effectsToCause (vericoins)

- Stephan Oeste (Emzy)
- Joe Bauers (joebauers)
- Jason Bisterfeldt (jbisterfeldt)
- Ed Leafe (EdLeafe)

Edizione Aperta

Questa è l'edizione aperta di "Mastering Bitcoin", pubblicata al fine di essere tradotta sotto licenza [Creative Commons Attribution Share-Alike License \(CC-BY-SA\)](#). Questa licenza ti permette di leggere, condividere, copiare, vendere, o riusare parti di questo libro, se tu:

- Applica la stessa licenza (Share-Alike)
- Include attribuzione

Attribuzione

Mastering Bitcoin di Andreas M. Antonopoulos LLC <https://bitcoinbook.info>

Copyright 2016, Andreas M. Antonopoulos LLC

Traduzione

Se stai leggendo questo libro in una lingua diversa dall'Inglese, sappi che è stato tradotto da volontari. Le seguenti persone hanno contribuito a questa traduzione:

- Francesco Canessa (<https://github.com/makevoid>)
- Gianmaria Allisiardi
- -